Risk Management Framework (RMF) Standard

1. Purpose

   Manage risk at the information system level for the State of Montana using the National Institute of Standards and Technology (NIST) Special Publication 800-37 Risk Management Framework (RMF).[1]

   The RMF process will result in a System Security Plan (SSP) with a supporting Body of Evidence (BoE), an authorization decision, and continuous monitoring associated with each State of Montana information system being managed for risk.[2]

2. Policy

   RMF applies to the following policies found within the Montana Operations Manual.
   a. Information Security Policy

3. Recommended Best-Practices to be Adopted as Standard Practice
   a. Implement the following NIST RMF six step workflow for all State of Montana information systems whether defined as stand-alone disconnected from State of Montana enterprise network (SummitNet), connected to SummitNet, or comprise the architecture supporting SummitNet.
      - Step 1 Categorize Information System
      - Step 2 Select Security Controls
      - Step 3 Implement Security Controls
      - Step 4 Assess Security Controls
      - Step 5 Authorize Information System
      - Step 6 Monitor Security Controls

   b. The RMF applies to all State of Montana information systems that are purchased externally, developed internally, or currently operational.

   c. All hardware or software procured for use in a State of Montana information system must be associated with an SSP. Risk associated with that hardware or software will be managed by the RMF process after procurement.

[1] NIST SP800-37; "*Guide for Applying the Risk Management Framework to Federal Information Systems*"; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf
[2] SSP and BoE are defined in the NIST "*Glossary of Key Information Security Terms*"; https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

d. All external cloud services procured for use as a State of Montana information system must be associated with an SSP. Risk associated with that cloud service will be managed by the RMF process after procurement.

e. Roles identified by NIST that are responsible for accomplishing each step of the RMF are defined in the Information Security Policy – Appendix B Roles and Responsibilities. Organizations must align the NIST RMF roles with similar (or complementary) State of Montana defined roles. For the State of Montana, minimum key roles will be aligned as follows:

- The Head of Agency is the Authorizing Official (AO) for that agency but may delegate another senior official as the AO for that agency.
- The Chief Information Officer (CIO) for the State of Montana is the AO for the Department of Administration.
- Agency Heads that delegate an AO for their agency must submit that delegation in writing to the CIO for the State of Montana.
- The AO for an agency may only authorize that agency's system to operate in a standalone mode or on a network owned by that agency
- The CIO for the State of Montana is the AO for SummitNet.
- Any system owned by any agency must receive an authorization from the CIO for the State of Montana to be connected to SummitNet.
- The Chief Information Security Officer (CISO) for the State of Montana is the Senior Information Security Officer (SISO) for the State of Montana.
- The SISO for an agency is the CIO for that agency or an equivalent position that meets the SISO criteria defined in Attachment 1.
- The Information Security Manager (ISM) role, codified in Montana law, for an agency is the same as the SISO role for an agency.[3]
- The SISO for an agency may delegate the ISM responsibilities to an Information System Security Officer (ISSO) for the agency.
- The Authorizing Official Designated Representative role will be known as the Delegated Authorizing Official (DAO) in the State of Montana RMF process.

[3] The ISM role is identified in MCA 2-15-114 "*Security Responsibilities Of Departments For Data*"; https://leg.mt.gov/bills/mca/title_0020/chapter_0150/part_0010/section_0140/0020-0150-0010-0140.html

4. Compliance

Compliance shall be evidenced by each agency implementing the best practices standards above and the Information Security Bureau managing implementation and evolution through an enterprise Information Security Program for the State of Montana. Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this RMF Standard are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.